UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/739,839	12/20/2000	Yusuke Kawasaki	1080.1088/JDH	3883

21171 7590 03/06/2008

STAAS & HALSEY LLP
SUITE 700
1201 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER	
HENNING, MATTHEW T	
ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
03/06/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	09/739,839	KAWASAKI ET AL.	
	Examiner	Art Unit	
	MATTHEW T. HENNING	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 December 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4,6-11,13-23,25-29 and 31-36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4,6-11,13-23,25-29 and 31-36* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *10 March 2006* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

This action is in response to the communication filed on 12/09/2007.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 12/09/2007 has been entered.

Response to Arguments

Applicants' arguments filed 12/09/2007 have been fully considered but they are not persuasive.

Regarding applicants' argument that the relied upon prior art does not teach or suggest supplying multiple clocks operating within a internal circuit, the examiner does not find the argument persuasive. First, the claim language does not specifically state that the first and second clocks are separate clocks. Second, based upon the teachings of Millhaupt, with regards to element 180 of Fig. 5, there are multiple clocks in the system. For example, in Fig. 5 Millhaupt, there are at least three different clocks from element 180. There is CLKA, CLKC, and CLK. Millhaupt teaches throttling back the processor clock when the processor is idle, in order to reduce power consumption. It therefore would have been obvious, based upon the teachings of Millhaupt, that in the combination as relied upon, when the data processing means is idle, but the encryption and decryption means are not idle, the clock to the data processing means

should throttled down to reduce power consumption, while the clock to the non-idle encryption/decryption means remains active. This would have been obvious because the ordinary person skilled in the art would have been motivated to reduce the power consumed by the data processor while the processor was idle and waiting for the software to be re-encrypted and stored in memory. Furthermore, it would have been obvious that a separate clock would need to be provided to the encryption/decryptions means in order for it to remain active while the data processing means' clock was throttled back. As such, the examiner does not find the argument persuasive.

Regarding applicants' argument that the initialization operation of the relied upon prior art is not an initialization operation when the device is first powered on. First, the examiner points out that although the applicants appear to argue that the initialization operation is executed when the device is first powered on, the examiner points out that this has not been claimed. Rather, it is claimed that the initialization operation is an initialization operation when the device is first powered on. As such, the examiner points out that operation must be programmed into the device and when the device is powered on, this programmed initialization operation is an initialization operation. As such, the examiner does not find the argument persuasive.

Claims 1-4, 6-11, 13-23, 25-29, and 31-36 have been examined.

All objections and rejections not set forth below have been withdrawn.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject

matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 11, 13-17, 19, 29, and 31-36 rejected under 35 U.S.C. 103(a) as being unpatentable over Taguchi et al. (U.S. Patent Number 5,915,025) hereinafter referred to as Taguchi, and further in view of Curran et al. (U.S. Patent Number 4,525,599) hereinafter referred to as Curran, and further in view of Schneier (Applied Cryptography: Second Edition).

Regarding claim 11, 29, and 36, Taguchi disclosed an internal circuit (See Taguchi Fig. 31 the Elements within Element 150) comprising a CPU executing programs (Element 151), at least one internal device having a predetermined function (Elements 152-157) and a bus line extending internally of the internal circuit (See connection from 153 and 154 to 160, and Col. 25 Lines 44-51, Col. 21 Lines 18-28, Col. 10 Lines 50-62, and Col. 9 Lines 49-65 especially lines 61-63) and connecting said CPU to said internal device (See connection from 151 to 153 and 154) the bus line comprising an externally extending portion extending externally of said external circuit (See connection from 153 and 154 to 160, and Col. 25 Lines 44-51, Col. 21 Lines 18-28, Col. 10 Lines 50-62, and Col. 9 Lines 49-65 especially lines 61-63) and transferring an address and data (See Col. 8 Lines 55-59), wherein said internal circuit includes at least one internal memory as an internal device (See Taguchi Fig. 31 Element 155 and Col. 13 Paragraphs 2-4 wherein it is disclosed that the key supply stores keys and retrieves keys upon request. Further see Taguchi Col. 2 Line 55 Col. 3 Line 55 wherein it was disclosed that processors had cache memory), the internal circuit including selection means for determining ciphering patterns (See Taguchi Col. 4 Paragraph 4 and Col. 22 Paragraph 3).

Taguchi further disclosed an external circuit (Elements 161-166) provided externally of the internal circuit and connected with the externally extending portion of said bus line (See all elements below 160) and including at least one external device having a predetermined function (Elements 161-166), wherein said external circuit includes at least one external memory as an external device (See Taguchi Fig, 31 Element 161 and Col. 8 Lines 33-36 wherein it was disclosed that the external storage was RAM (Random Access Memory)).

Taguchi also disclosed that the internal circuit comprises a ciphering section (Element 153) interposed at an entrance to an external side of said internal circuit (See connection from 153 to 160, and Col. 25 Lines 44-51, Col. 21 Lines 18-28, Col. 10 Lines 50-62, and Col. 9 Lines 49-65 especially lines 61-63) and ciphering the data on the bus line by ciphering patterns according to a plurality of regions divided from an address space allotted to entirety of said at least one external device (See Col. 8 Paragraph 5).

Taguchi further disclosed that the ciphering patterns include at least one pattern in which neither the address nor the data is enciphered (See Taguchi Col. 14 Paragraph 1 and Col. 20 Paragraph 45-56 wherein the encryption being performed was a basic XOR and the encryption keys were chosen randomly. In this case, that the random key could be a string of all zeros, and XORing data with all zeros does not encrypt the data.)

Taguchi further disclosed that the internal circuit has information rewrite means for ciphering and rewriting at least part of the information stored in said external memory in a predetermined initialization operation, to thereby prevent illicit access to the internal memory via the external memory (See Taguchi Fig. 12 and Fig. 13).

However, Taguchi failed to disclose the ciphering of the address. Taguchi also failed to specifically state that the processing means was provided with cache memory, but Taguchi did imply that the cache memory was there (See Taguchi Col. 2 Line 55 Col. 3 Line 55). Further, Taguchi failed to specifically disclose that the system bus comprised both an address bus and a data bus. Further still, Taguchi failed to disclose that the selection means included a program stored in internal memory for determining the ciphering patterns. Even further still, Taguchi did not specifically disclose that the initialization operation was an initialization operation when the apparatus is first powered on.

Curran teaches that software can be protected from illegal copying by encrypting the addresses of the data being accessed in order to provide a non-sequential ordering of the data in memory as well as encrypting the data stored therein (See Col. 1 Paragraph 5 – Col. 2 Paragraph 1 and Col. 3 Paragraph 3).

Schneier teaches that any encryption algorithm can be implemented in software in order to provide flexibility, portability, ease of use, and ease of upgrade (See Schneier Page 225 Lines 24-43).

Furthermore, it was well known in the art at the time of invention that processors accessed data directly from cache memory and external storage, such as RAM, accessed the data from the cache memory (See Taguchi Col. 2 Line 55 Col. 3 Line 55). It therefore would have been obvious to the ordinary person skilled in the art at the time of invention to employ what was known in the art at the time of invention to the processing system of Taguchi by storing data to be input and output by the processing means in cache memory. This would have been obvious because the ordinary person skilled in the art would have been motivated to decrease the access

time to the data. In this combination, illicit access to the data in the cache would be prevented because the data sent out of the internal circuit from the cache would be encrypted (See Taguchi Col. 8 Paragraph 5).

It was further well known in the art at the time of invention that busses comprised an address bus, data bus, and control bus and therefore it would have been obvious to the ordinary person skilled in the art for the system bus of Taguchi to incorporate all three as well.

It also would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Curran to the invention of Taguchi in order to encrypt the addresses as well as the data on the external bus. This would have been obvious because the ordinary person skilled in the art would have been motivated to further protect the software and other data stored external from the data processor from illicit access.

It further would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Schneier in the software protection apparatus of Taguchi and Curran by implementing the encryption method selection means 157 in software. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide flexibility, portability, ease of use, and ease of upgrade of the selection means. It further would have been obvious that the software would have been stored in memory in the protection apparatus in order for it to have been used by the protection apparatus (See Taguchi Fig. 31 Element 157).

Further, in this combination, it would have been obvious to have the device programmed/configured with the key updating routine and re-encryption routines prior to the devices being first powered on. This would have been obvious because the ordinary person

skilled in the art would have been motivated to prevent needing to update the device to provide this functionality to the device at a later time.

Regarding claims 13 and 31, Taguchi and Curran and Schneier disclosed that the information rewrite means generates a random number, and performs ciphering by adopting a ciphering pattern using the generated random number (See Taguchi Col. 14 Lines 4-6).

Regarding claims 14-17 and 32-35, see Taguchi Col. 21 Paragraphs 5-6.

Regarding claim 19, Taguchi and Curran and Schneier disclosed that the internal circuit holds a ciphering pattern adopted by said ciphering section (See Taguchi Fig. 31 Element 155), the processing apparatus further comprises a tamper detection section detecting tamper, and ciphering pattern destruction means for destroying the ciphering pattern held in said internal circuit in response to tamper detection made by said tamper detection section (See Col. 9 Paragraph 2).

Claims 1-3, 6-10, 21-22, and 25-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Taguchi and Curran and Schneier as applied to claims 1 and 20 respectively above, and further in view of Milhaupt et al. (U.S. Patent Number 5,706,445) hereinafter referred to as Milhaupt.

The combination of Taguchi and Curran and Schneier disclosed the use of a processor and a separate encryption circuit (See Taguchi Fig. 31), but failed to disclose using separate clocks with the encryption clock being set at a higher frequency than the processor clock. However, Taguchi and Curran and Schneier did disclose that when encrypted software was input

to the system at the CD-ROM drive (See Taguchi Fig. 31) the decryption means had to decrypt the software and then the encryption means had to encrypt the software and store the software in memory before the processor could access the software (See Taguchi Col. 10 Paragraph 1).

Milhaupt teaches that reducing the clock rate to the processor during times when the processor is not being used can dramatically reduce the power consumed by a processor (See Millhaupt Fig. 5 and Col. 8 Lines 52-53 and Col. 11 Paragraph 2).

It would have been obvious to the ordinary person skilled in the art to employ the teachings of Milhaupt in the combination of Taguchi and Curran and Schneier by providing each portion of the device with a separate clock which can be throttled back when the portion is idle, and further to throttle back the clock of the processing means when the processing means is idle and the encryption/decryption means is active. This would have been obvious because the ordinary person skilled in the art would have been motivated to reduce the power consumed by the data processor while the processor was idle and waiting for the software to be re-encrypted and stored in memory.

Regarding claims 2 and 21, see the rejection of claim 11 above.

Regarding claims 3 and 22, Taguchi and Curran and Schneier and Millhaupt disclosed that the external circuit includes a plurality of external devices (See Taguchi Fig. 31 Elements 161-166), and said ciphering section performs ciphering using ciphering patterns according to said plurality of external devices, respectively (See Taguchi Fig. 15).

Regarding claims 6 and 25, Taguchi and Curran and Schneier and Millhaupt disclosed that the ciphering pattern determination means for recognizing a constitution of said external

circuit and determining a ciphering pattern of said ciphering section according to the constitution of said external circuit (See Taguchi Col. 9 Paragraph 5 – Col. 10 Paragraph 1).

Regarding claims 7 and 26, Taguchi and Curran and Schneier and Millhaupt disclosed that the said ciphering section ciphers the address and the data on said bus line by ciphering patterns according to the plurality of regions divided from the address space allotted to the entirety of said no less than one external device and according to application programs executed by said CPU (See Fig. 15 and Col. 8 Lines 55-63).

Regarding claim 8, Taguchi and Curran and Schneier and Millhaupt disclosed a deciphering section connected to the externally extending portion of said bus line, and returning the ciphered address and the data on the bus line to an address and data which are not ciphered (See Taguchi Fig. 31 Element 154 and Col. 10 Lines 25-27).

Regarding claims 9 and 27, Taguchi and Curran and Schneier and Millhaupt disclosed ciphering pattern change means for changing a ciphering pattern whenever a predetermined initialization operation is carried out for one of the plurality of regions divided from the address space allotted to the entirety of said at least one external device (See Taguchi Fig. 11, Fig. 13, and Fig. 15).

Regarding claims 10 and 28, Taguchi and Curran and Schneier and Millhaupt disclosed that the ciphering section adopts a ciphering pattern in which ciphered data is changed according to the address, for one of the plurality of regions divided from the address space allotted to the entirety of said at least one external device, to thereby cipher the data (See Taguchi Fig. 11, Fig. 13, and Fig. 15).

Regarding claim 18, Taguchi and Curran and Schneier and Millhaupt disclosed that the internal circuit holds a ciphering pattern adopted by said ciphering section (See Taguchi Fig. 31 Element 155), the processing apparatus further comprises a tamper detection section detecting tamper, and ciphering pattern destruction means for destroying the ciphering pattern held in said internal circuit in response to tamper detection made by said tamper detection section (See Col. 9 Paragraph 2).

Claims 4 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Taguchi and Curran and Schneier and Millhaupt as applied to claims 1 and 20 respectively above, and further in view of IBM (IBM Technical Disclosure Bulletin 19800601).

The combination of Taguchi and Curran and Schneier and Millhaupt disclosed the use of random number in generating keys (See Taguchi Col. 14 Lines 4-6), but the combination of Taguchi and Curran and Schneier and Millhaupt failed to disclose any information regarding times when the external bus was not being used.

IBM teaches that memory can be tested by generating random addresses, storing random data to the random addresses, and then checking that the generated data and the stored data are consistent.

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of IBM in the combination of Taguchi and Curran and Schneier and Millhaupt in order to test the memory when the external bus was not in use. This would have been obvious because the ordinary person skilled in the art would have been motivated to ensure that the external memory was working properly, thus ensuring data integrity.

Conclusion

Claims 1-4, 6-11, 13-23, 25-29, and 31-36 have been rejected.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MATTHEW T. HENNING whose telephone number is (571)272-3790. The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Matthew Henning
Assistant Examiner
Art Unit 2131
2/26/2008

/Ayaz R. Sheikh/
Supervisory Patent Examiner, Art Unit 2131